GOTO
AARHUS 2023

#GOTOaar

goto;

Has my IoT device been 

ESTABLISHING TRUST WITH REMOTE ATTESTATION

Edlira Dushku
Assistant Professor in Cyber Security
Aalborg University, Copenhagen, Denmark
edu@es.aau.dk

A bit about me

Edlira Dushku

IoT Security, Trusted Computing

- **(2016 - 2020): PhD** *at Sapienza University of Rome, Italy*
- **(2020 – 2022): Postdoc** *at Technical University of Denmark (DTU)*
- **November 2022: Assistant Professor** *at Aalborg University*

Content

- Internet of Things Security
- Remote attestation protocols
- Open challenges

Content

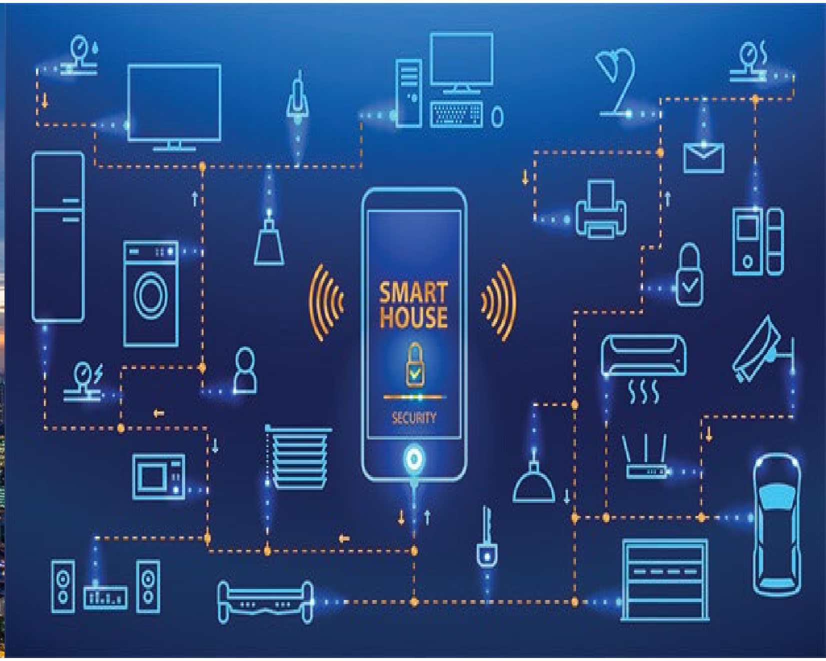
- **Internet of Things Security**
- Remote attestation protocols
- Open challenges


Smart society
Smart healthcare
Smart transport
Smart territory improvement
Smart payments
Smart buildings
Smart energy
H

Internet of Things (IoT) systems

Industrial IoT

IoT for instrustructure



Consumer IoT

goto;

Cyberattacks on Iran — Stuxnet and Flame

News about Cyberattacks on Iran — Stuxnet and Flame, including commentary and archival articles published in The New York Times.

About 90% of Smart TVs Vulnerable to Remote Hacking via Rogue TV Signals

Oct. 10, 2017

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

How Israel Caught Russian Hackers Scouring the World for U.S. Secrets

Exploiting the popular Kaspersky antivirus software, Russian hackers searched millions of computers for American intelligence keywords. Israeli intelligence tipped off American officials.

Over 8,600 vulnerabilities found…

FDA recalled half a million pacemakers…

"If you want to keep living, pay a ransom, or die…"

Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer

Sunday, April 15, 2018 Wang Wei

Share 9.13k Share Tweet Share

IoT devices prone to cyberattacks

goto;

EASY TO EXPLOIT

- Resource-constrained devices with low-cost design
- Do not support complex security techniques

ATTRACTIVE TARGET

- Deployed in safe-critical domains
- Contain sensitive data & control physical environment

AMPLIFY THE ATTACK IMPACT

- Many interconnected devices
- Spread quickly the malware

How to improve the situation?

Option 1: Security-by-design

Security-by-design

Security-by-~~design~~ magic

- No cybersecurity expert
- No additional time/money
- Rush to market

Option 1: Security-by-design

Difficult: Cannot guarantee that devices do not get compromised

Option 2: Malware detection

Detect compromised device (to isolate from the network)

How to detect malware presence?

Guarantee that the device is

“telling the truth”

even when it is infected by malware

Remote attestation (RA)

goto;

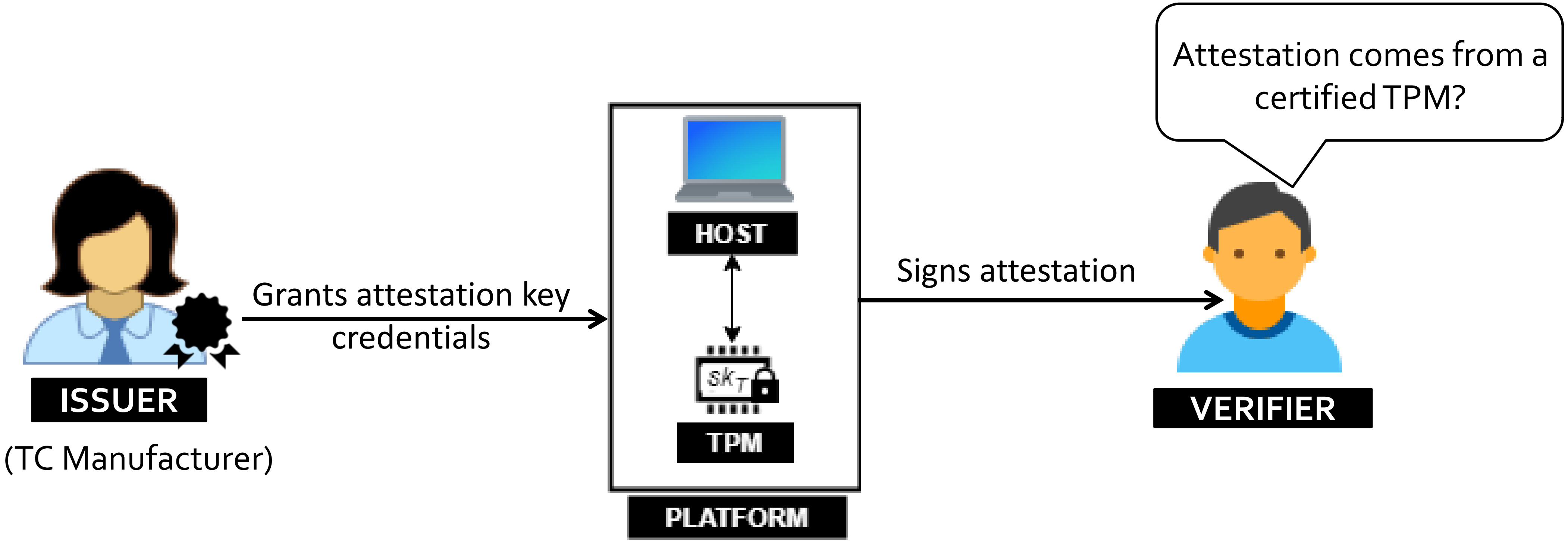
- Two-party Security Protocol
  - **Verifier**: an external trusted entity, not always present, not possible to physically reach a device
  - **Prover**: a (potentially) compromised device

- RA allows the **Verifier** to **guarantee** the **authentication and integrity** of the software running on **Prover**

- Verify that Prover is **NOW** running the initial application

RA in Traditional systems: TPM

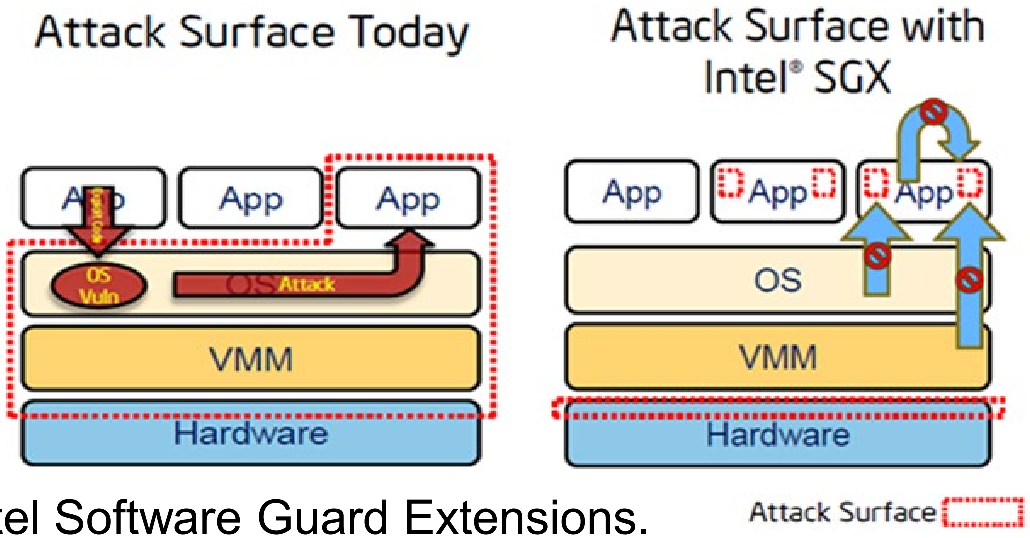
- **Hardware-based attestation** using a Trusted Platform Module (TPM)
- Secure crypto processor creates, stores, uses cryptographic keys
- Direct Anonymous Attestation (DAA): Makes anonymous remote attestations of host status



RA in Traditional systems: SGX

goto;

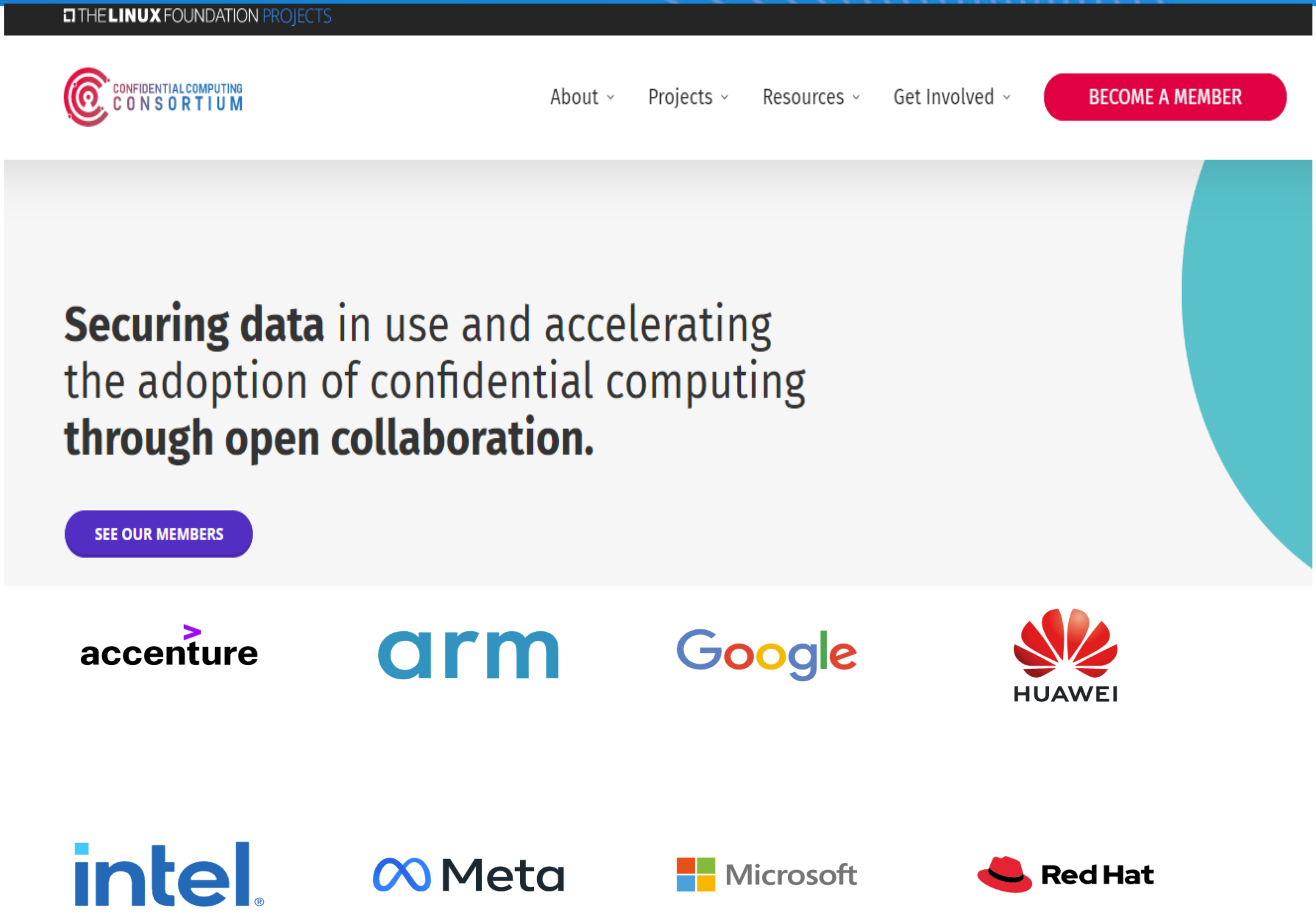
- Hardware-based memory encryption that isolates specific application code and data in memory.
- Allows user-level code to allocate private regions of memory, called enclaves, which are designed to be protected from processes running at higher privilege levels.



Intel Software Guard Extensions.
https://software.intel.com/en-us/sgx

Confidential Computing

goto;



https://confidentialcomputing.io/

Content

- Internet of Things Security
- **Remote attestation protocols**
- Open challenges

Overview of Remote attestation in IoT

1. Challenge (Executed by Verifier)

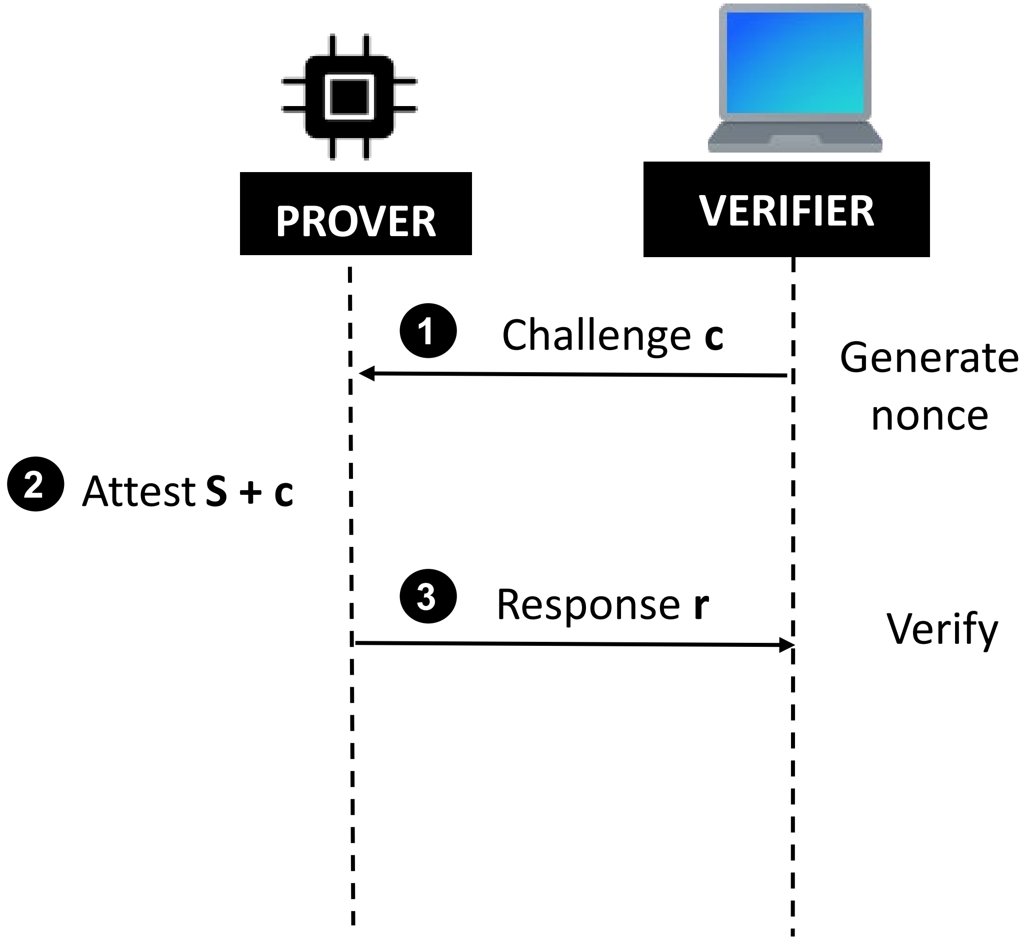
Outputs a random Challenge (nonce, timestamp, memory addresses, attestation routine)

2. Attest (Executed by Prover)

Computes a small attestation response based on internal state **S** (e.g., checksum over memory contents) and challenge **c**

3. Verify (Executed by Verifier)

Compares with the response received from Prover with the expected state



Typical adversary models

1. **Software Adversary**
    - **Remote:** Infect device(s) with malware
    - **Local:** Learn device secret, impersonate or clone, can launch side channel attack
    - **Mobile adversary:** Relocates or deletes itself
2. **Hardware Adversary**
    - **Stealthy Physical Intrusive:** Capture device and physically extract secrets, clone device(s)
    - **Physical Intrusive:** Capture device and modify contents/components

Requirements of Remote attestation

1. Challenge (Executed by Verifier)

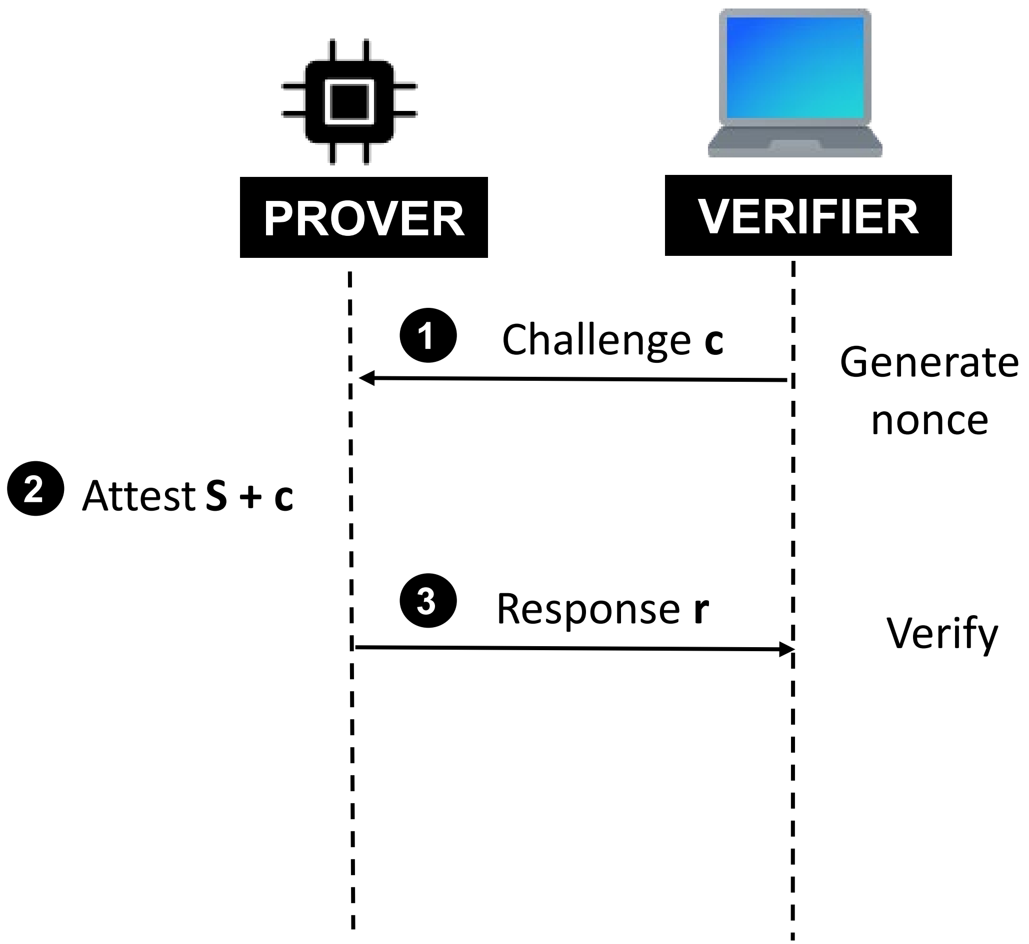
- Authentic, Fresh, Unpredictable

2. Attest (Executed by Prover)

- Authentic, Unforgeable, Dynamic, Deterministic

3. Verify (Executed by Verifier)

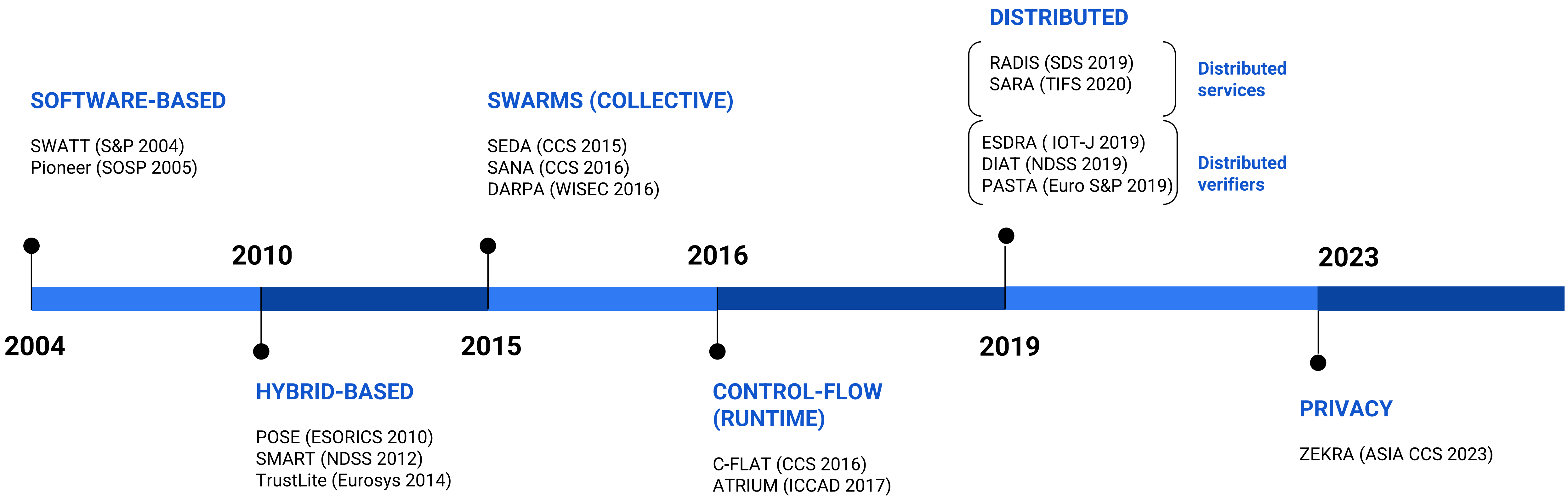
- Deterministic



Approaches of Remote attestation

- **Hardware design**
  Hardware-based, Software-based, or Hybrid
- **Memory**
  Static vs Control-flow attestation
- **Number of Device**
  Single Device vs Swarms (Collective)
- **Network Topology**
  Static vs Dynamic Swarms
- **Communication data**
  Swarms vs Distributed services

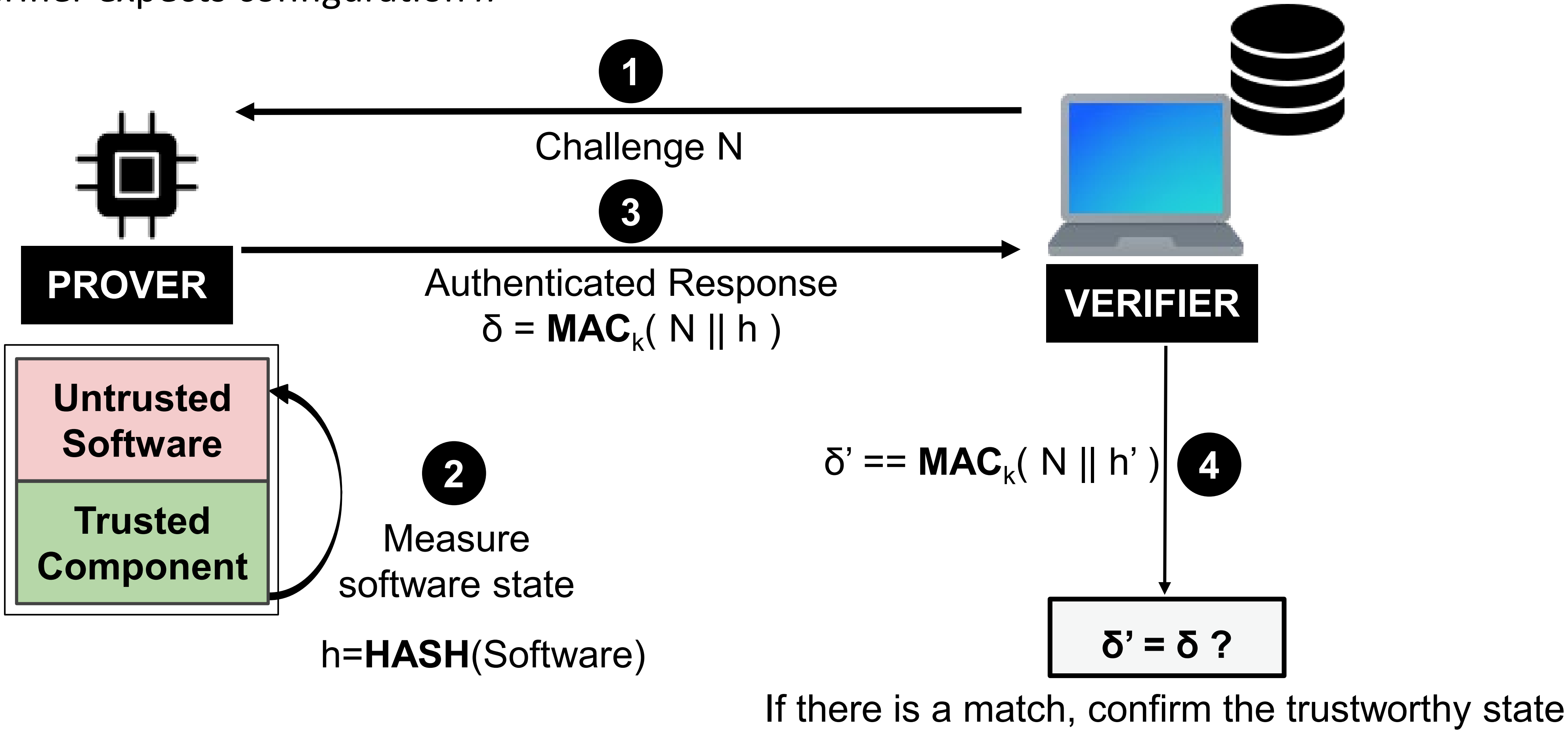
History of Remote attestation



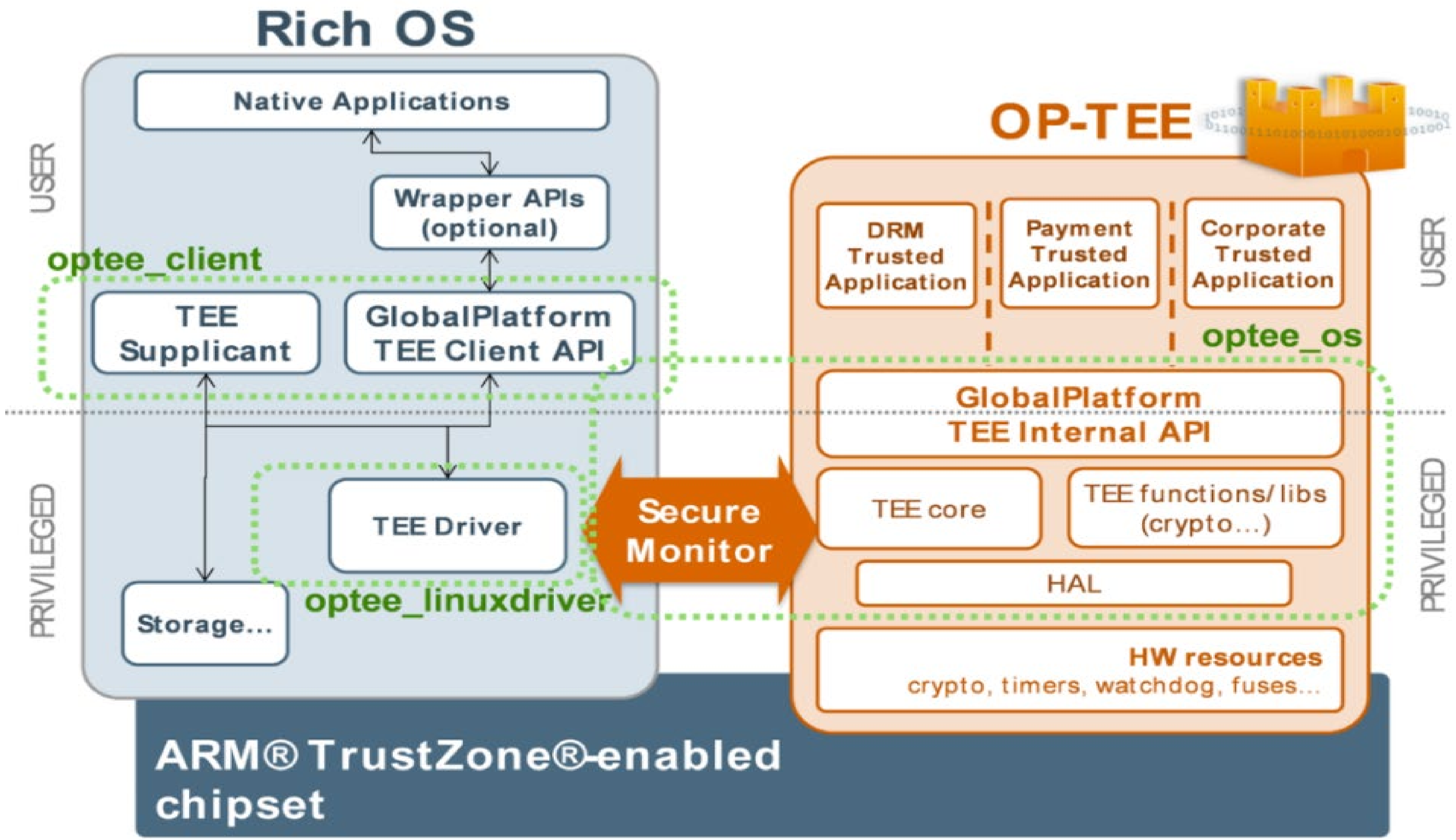
Hybrid attestation (Typical RA paradigm)

goto;

- Prover and Verifier share a key *k*
- Verifier expects configuration *h'*

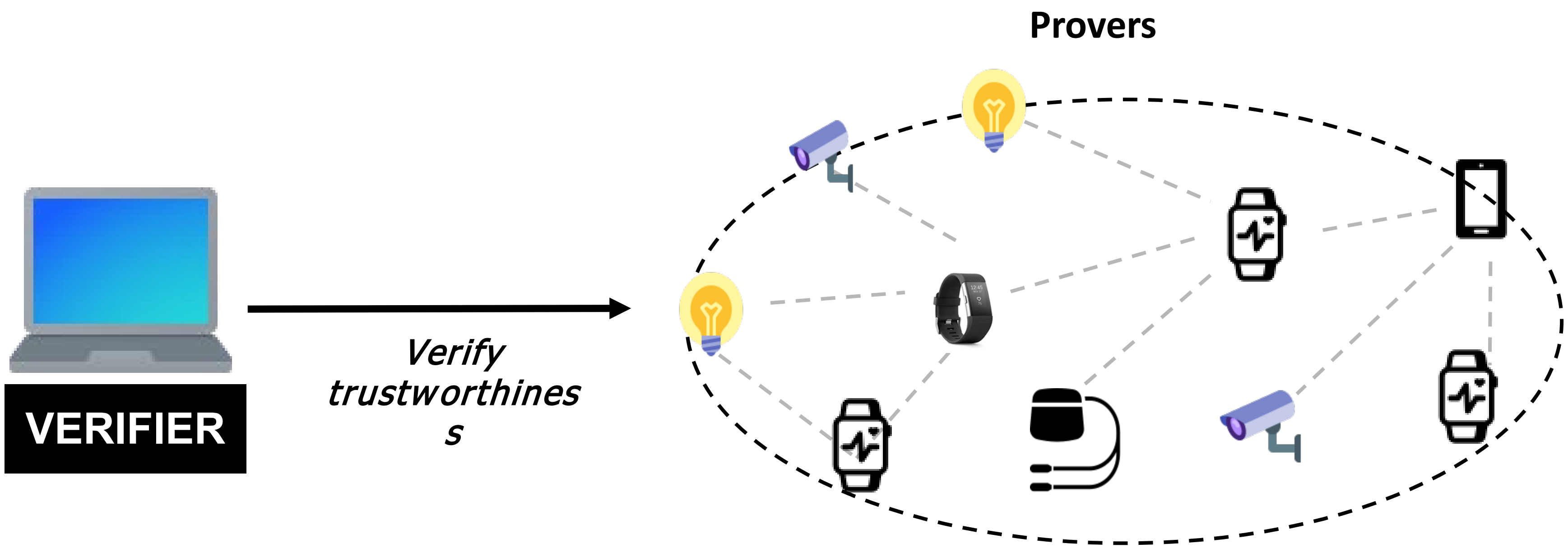


Arm TrustZone



Swarm attestation (Collective)

- Verify the internal state of a large group of devices
- Should be more efficient than attesting each node individually



Asokan, N., Brasser, F., Ibrahim, A., Sadeghi, A.R., Schunter, M., Tsudik, G.,Wachsmann, C.: **SEDA: Scalable embedded device attestation.** CCS ’15, New York, NY, USA, ACM (2015)

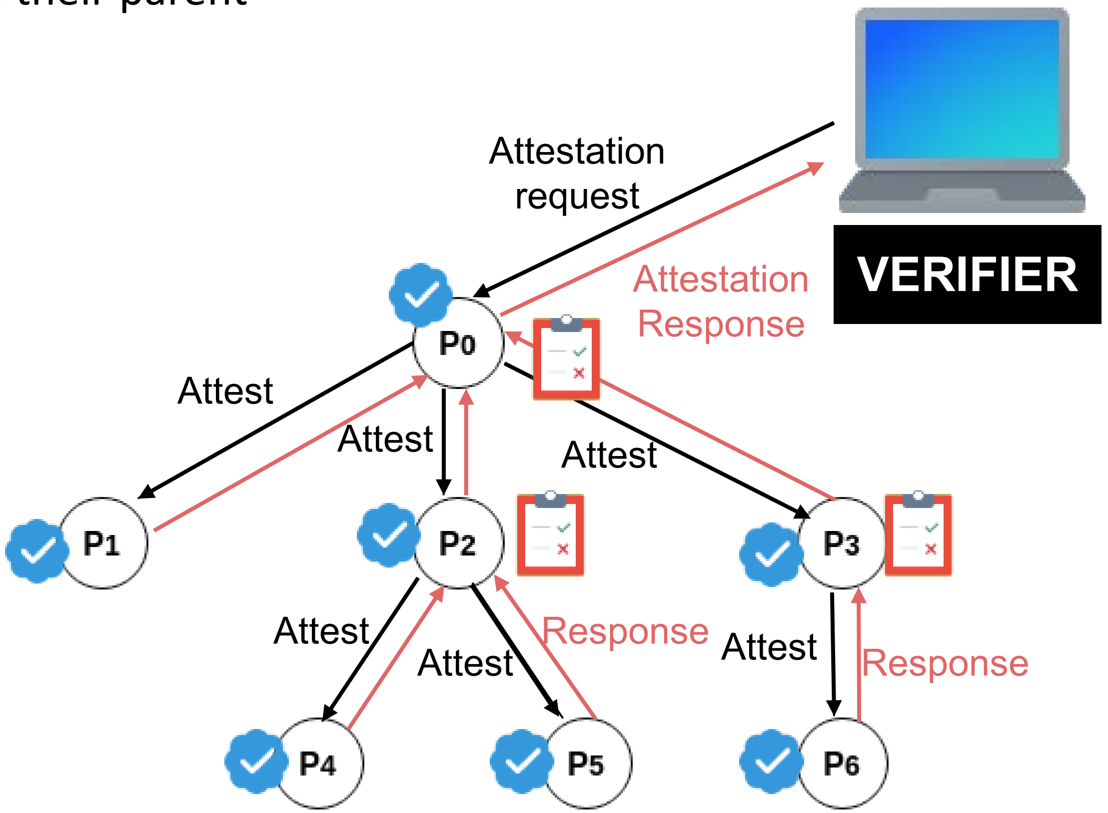
SEDA: Scalable Embedded Device Attestation

Algorithm logic:

1. Verifier selects random Prover (P_0) initializes attestation
2. Spanning tree is created rooted at P_0
3. Each Prover (device) gets attested by its parent (leaves first)
4. Sub-tree roots accumulate results and reports to their parent
5. P_0 reports overall result to Verifier

Aggregator

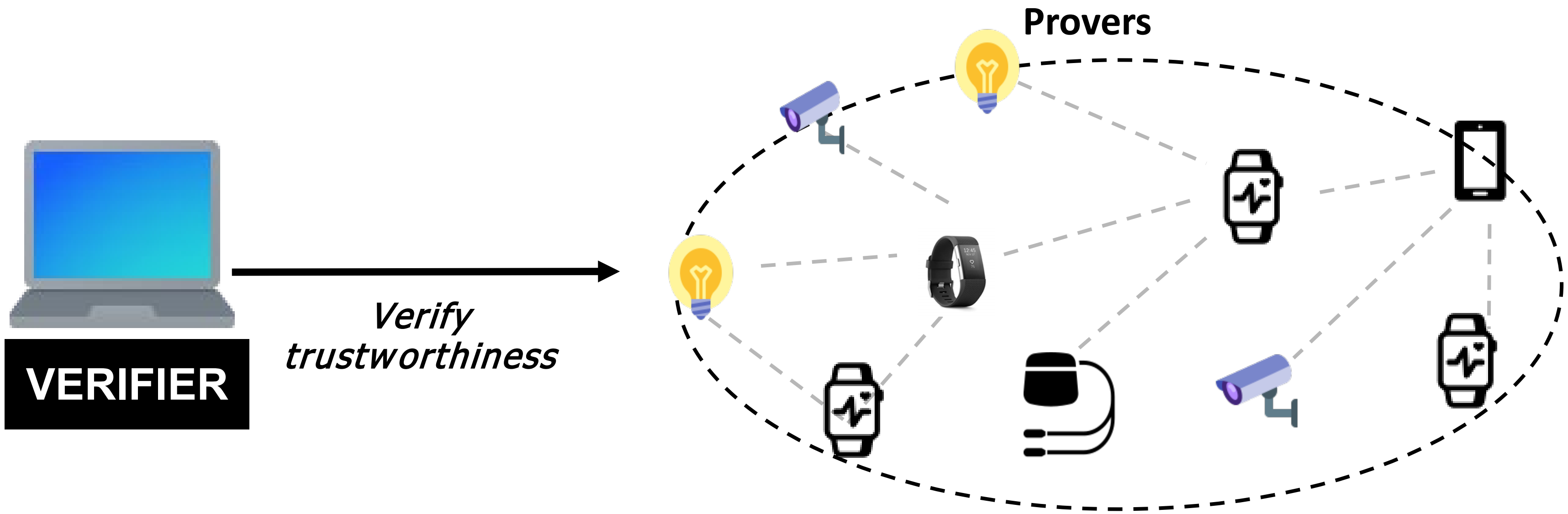
Attested Prover



SEDA: Scalable Embedded Device Attestation

Limitations

- Lack of flexibility (ALL devices must participate to attestation), final result is boolean
- Aggregators should be trusted, single point of failure
- Network topology and attestation are static



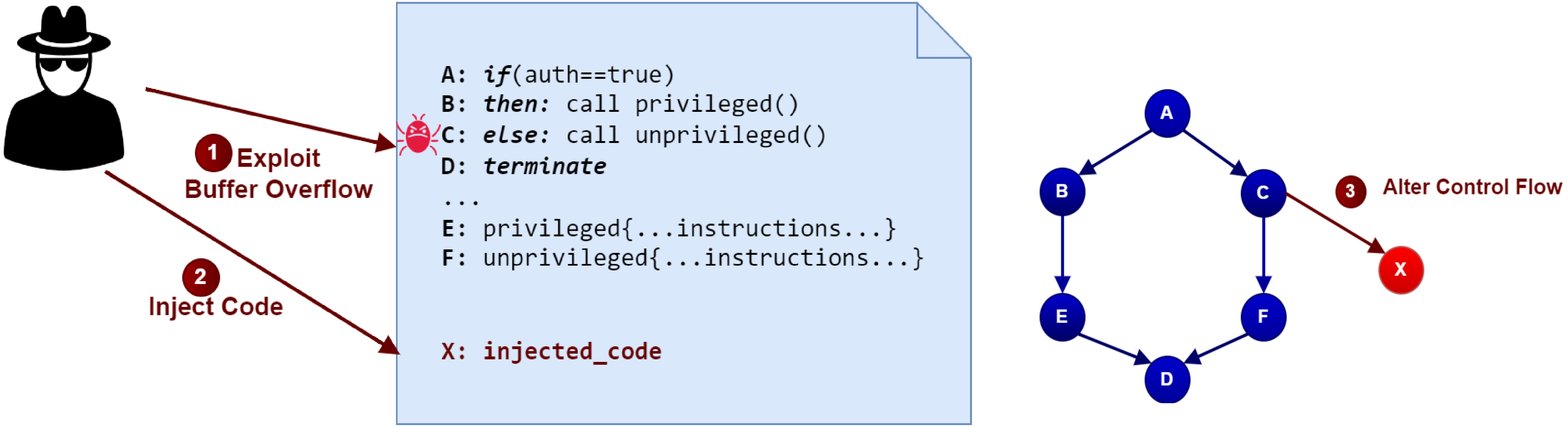
Dynamic attestation

Program Memory Attestation schemes

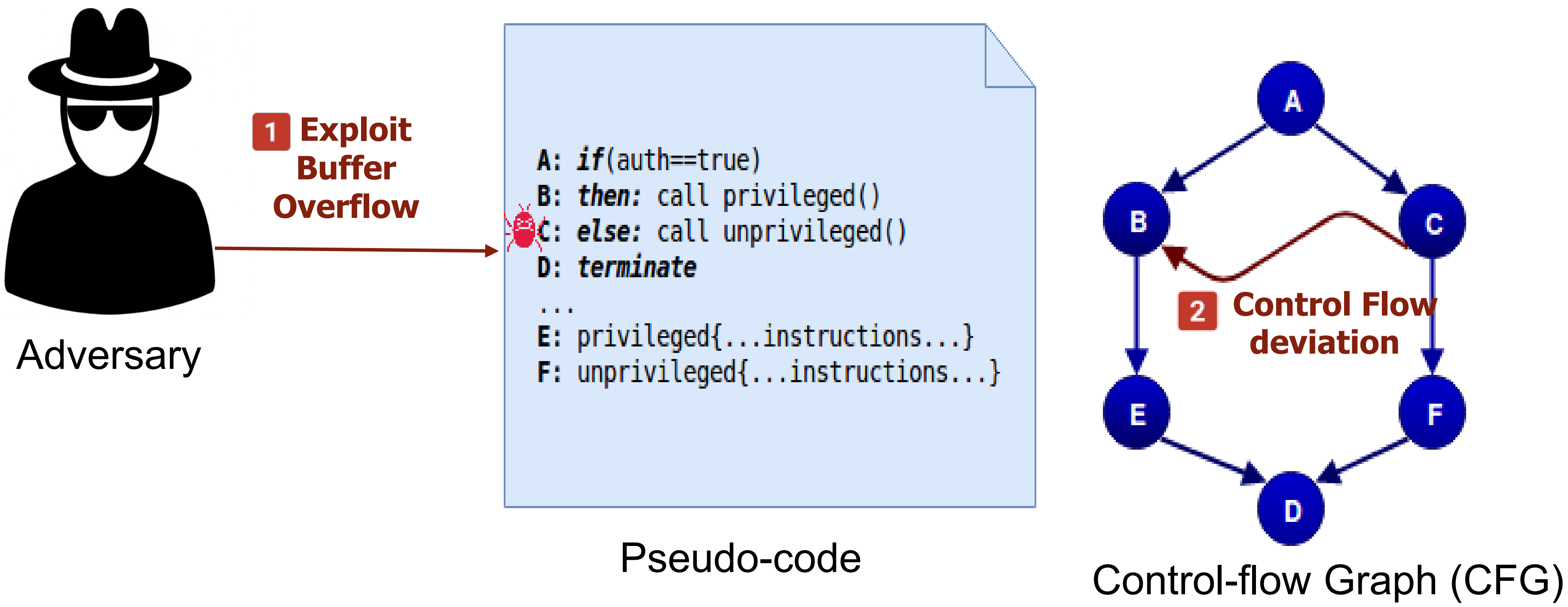
do not

address runtime attacks

Code injection attacks



Code reuse attack



C-FLAT: Control-flow attestation

goto;

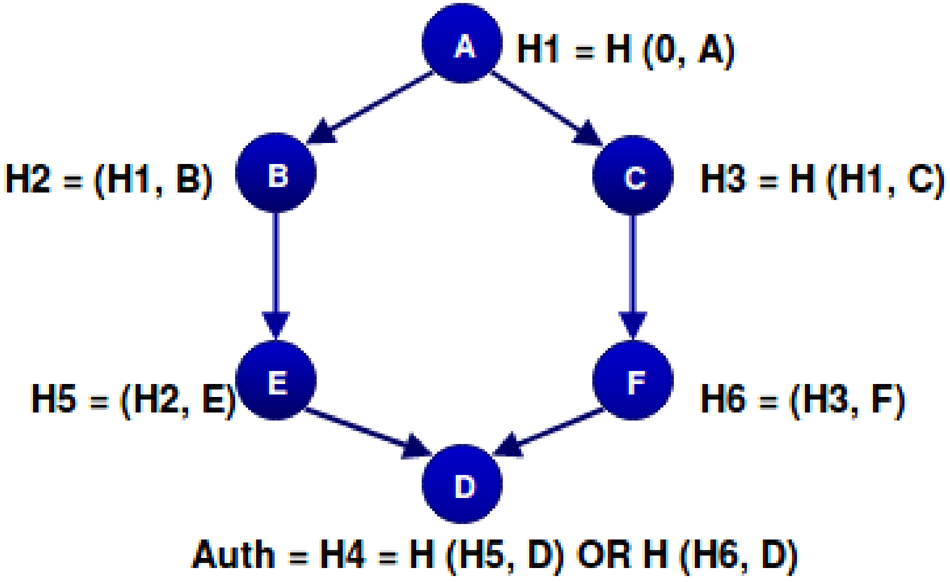
- Proposes a complete attestation of the run-time state of the Prover

- A single hash value that represents the entire control flow of the Prover’s state

Abera, T., Asokan, N., Davi, L., Ekberg, J.-E., Nyman, T., Paverd,A., Sadeghi, A.-R., and Tsudik, G.C-FLAT: Control-Flow Attestation for Embedded Systems Software. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security CCS ’16.(2016).

C-FLAT: Control-flow attestation

Cumulative Hash Value: Hi = H (H i-1 , N)
H i-1 -- previous hash result
N -- instruction block (node) just executed



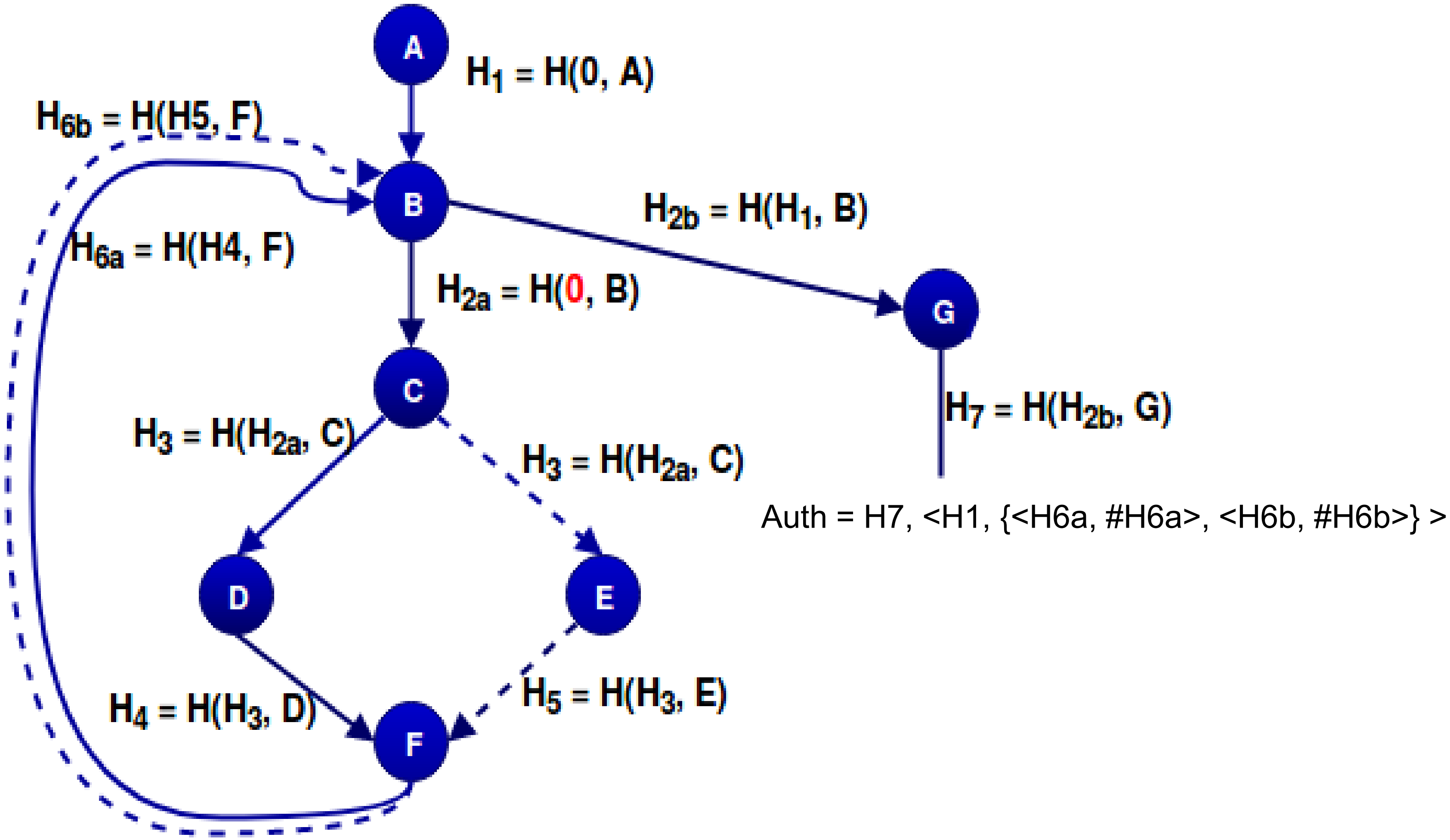
Loops are a challenge!

Different loop paths
and loop iterations lead to many valid
hash values

C-FLAT Approach:

Treat loops as sub-graphs
and report their hash values
and # of iterations separately

C-FLAT approach



Summary of Dynamic attestation

Advantages

- Better detection level: Detects runtime attacks

Disadvantages

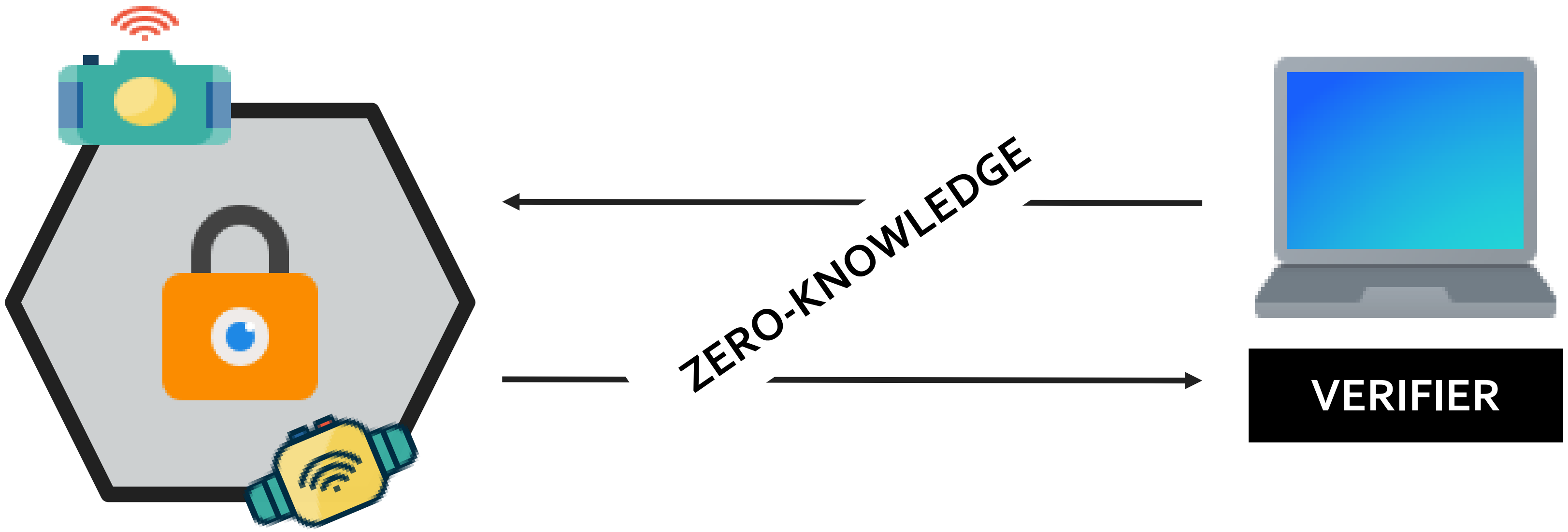
- The protocols rely on customized hardware support
- The computations are not efficient

Content

- Internet of Things Security
- Remote attestation protocols
- **Open challenges**

PRIVACY

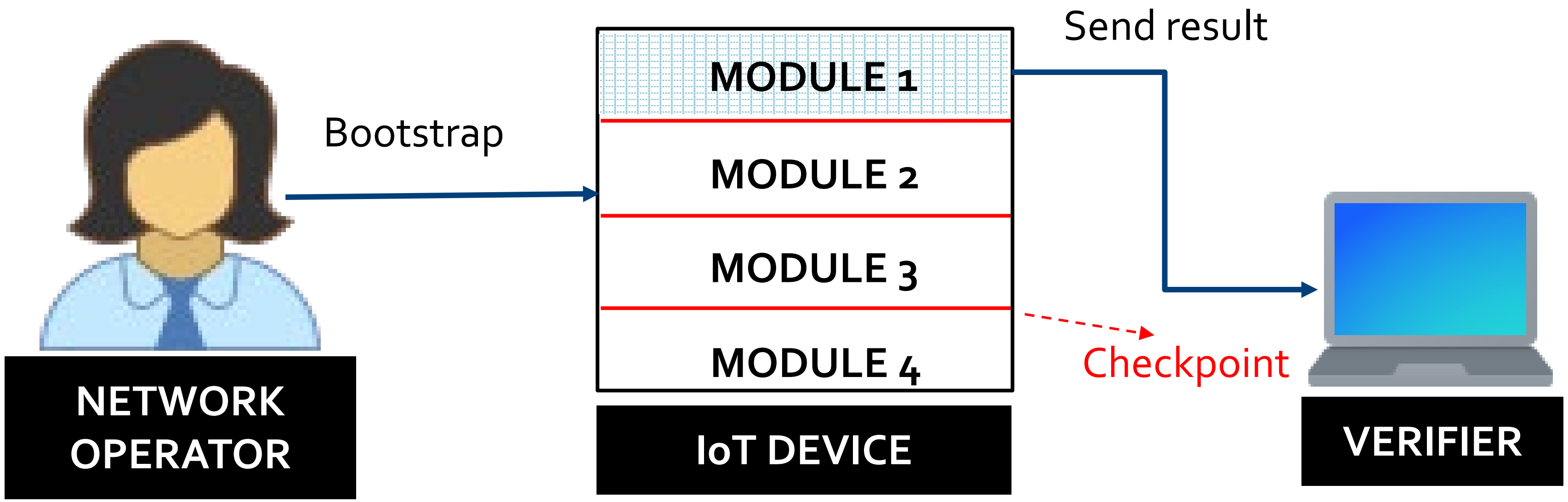
- Privacy-preserving remote attestation for IoT systems



ZEKRA: Zero-Knowledge Control-Flow Attestation.
Heini Bergsson Debes, Edlira Dushku, Thanassis Giannetsos, Ali Marandi,
To appear: the 18th ACM ASIA Conference on Computer and Communications Security (AsiaCCS 2023)

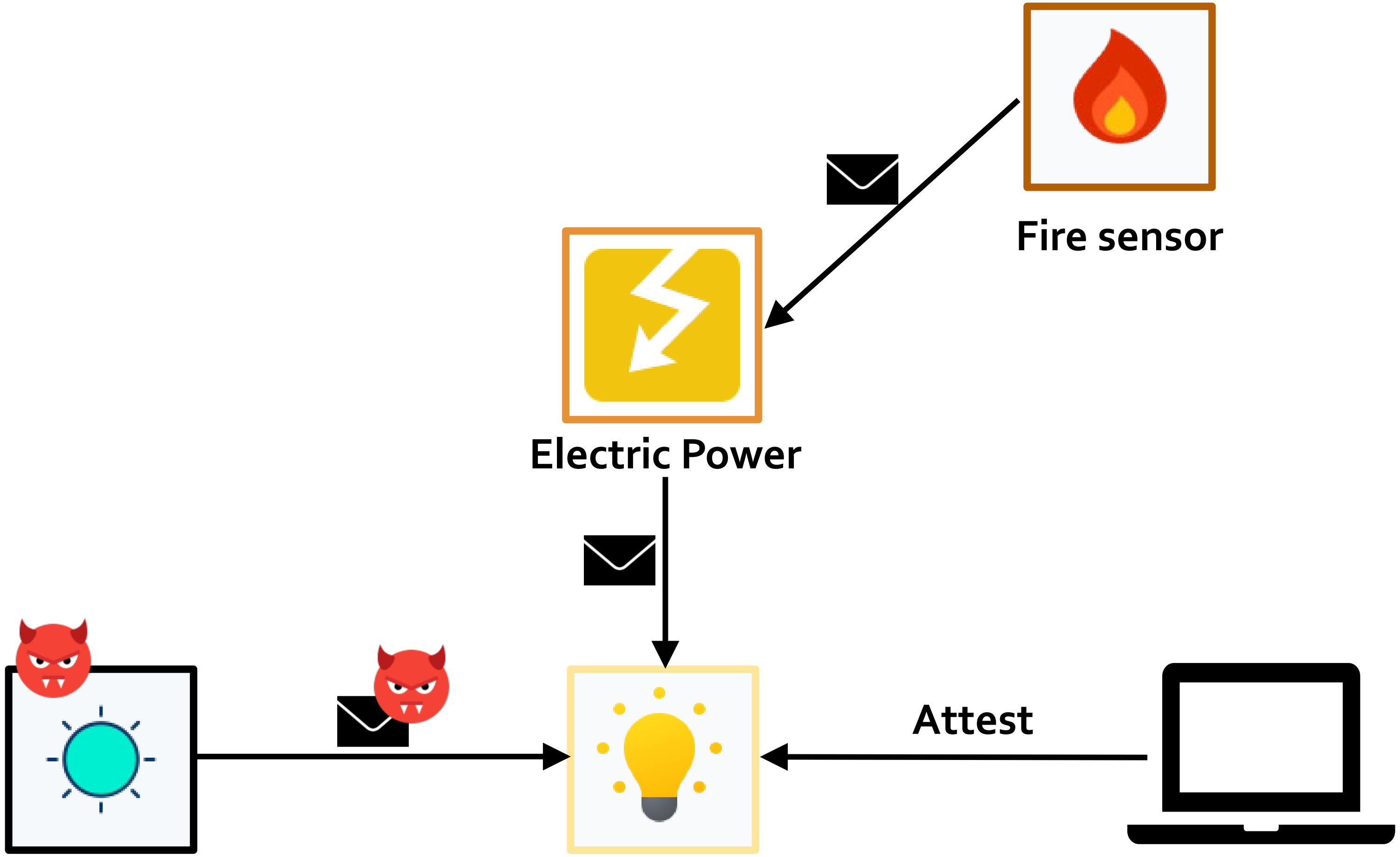
Energy-harvesting IoT security

- Lightweight RA operation designed specifically for Intermittent IoT system



RESERVE: Remote Attestation of Intermittent IoT devices
MD M. Rabbani, E. Dushku, J. Vliegen, A. Braeken, N. Dragoni, N. Mentens
In Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems (SenSys '21)

Asynchronous Swarm attestation



Dushku, E., Rabbani, M. M., Conti, M., Mancini, L. V., and Ranise,S. SARA: Secure Asynchronous Remote Attestation. In IEEE Transactions on Information Forensics and Security, vol. 15, pp.3123-3136, 2020..

Conclusions

goto;

- Introduced RA of IoT devices: Security protocol that guarantees trustworthiness
- Highlighted the need for the attestation of IoT devices. RA can serve as a fundamental building block for other security protocols.
- Presented an overview of the main RA protocols proposed in the literature (hybrid, swarm, control-flow)

Would you like to know more?

goto;

Grab a course at Master of IT

- Software construction
- Cyber Security
- IT-architecture
- Digital transformation
- Data Science
- IT-management

Read more

www.master-it-vest.dk

Winner of the Informatics Europe 2020 Best Practices in Education Award

It-vest samarbejdende universiteter

AARHUS UNIVERSITET

AALBORG UNIVERSITET

SDU

Thank you!

Edlira Dushku
edu@es.aau.dk

AALBORG UNIVERSITY